AO 106 (Rev. 04/10) Application for a Search Warrant

# UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

14856 Southeast Spanish Bay Drive, Happy Valley, Oregon, as further described in Attachment A

Case No. '19 -MC- 881



## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

14856 Southeast Spanish Bay Drive, Happy Valley, Oregon, as further described in Attachment A

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. §§ 1956, 1957, 1956(h) | Conspiracy to Commit Money Laundering; Money Laundering, Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity |

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

DEA Special Agent Justin Hussey
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 10/21/2019

*Judge's signature*

City and state: Portland, Oregon

Jolie A. Russo, United States Magistrate Judge
*Printed name and title*

# ATTACHMENT B

## Items to Be Seized

The items to be searched for, seized, and examined, are those items on the premises located at 14856 Southeast Spanish Bay Drive, Happy Valley, Oregon (the **Target Residence**), referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of *Conspiracy to Commit Money Laundering*, in violation of 18 U.S.C. §§ 1956, 1957 and 1956(h); *Money Laundering*, in violation of 18 U.S.C. § 1956; and *Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity*, in violation of 18 U.S.C. § 1957. The items to be seized cover the period of February 1, 2016 through the date of the execution of the search warrant.

1. **The items referenced to be searched for, seized, and examined are as follows**:

a. Controlled substances, including but not limited to fentanyl and its analogues (powder and/or pressed into pills);

b. Firearms and other dangerous weapons and ammunition;

c. Financial profits, proceeds and instrumentalities of money laundering, and financial profits and proceeds of trafficking in narcotics, including U.S. Currency and other items of value;

d. Books, records, receipts, notes, ledgers, and other documents relating to money laundering, the manufacture and distribution of controlled substances, communications between members of the conspiracy, and evidence of the use of apparently legitimate businesses to disguise profits;

e. Personal books and papers reflecting names, addresses, telephone

numbers, and other contact or identification data relating to money laundering;

f. Financial records relating to money laundering, proceeds of controlled substances, and expenditures of money and wealth, to wit: money orders, wire transfer records, cashier's checks and receipts, account records, passbooks, tax records and related tax preparation files including schedules, safe deposit box keys and records, checkbooks, check registers, cancelled checks, deposit slips, loan documents, credit card records, receipts and records related to gambling wins and losses, or any other contest winnings, receipts for items of value, documents relating to purchase of vehicles including RVs, vehicle and title documents, insurance documents for real property and other items of value such as vehicles, profit and loss statements, accounting work papers, income and expense ledgers, negotiable instruments, stored value/prepaid cards, receipts for the purchases and expenditures made on stored value/prepaid cards, records showing employment or lack of employment, money bands for currency, money counters, and jewelry, watches, precious metals and gems such as gold, silver, diamonds, etc;

g. Real property records including papers, documents, information, or other records, such as real estate purchase and sale agreements, HUD-1 statements, loan applications, and supporting documents, financial statements, security agreements, loan commitments sheets, earnest money agreements, credit reports, loan payment ledgers, quit claim deeds, excise tax affidavits, warranty deeds and deeds of trust, internal application forms or other notes relating to information necessary to fill out these documents, and similar records of other property owned or rented;

h. Evidence of personal property ownership including registration information, ownership documents, purchase documents, or other evidence of ownership of

property including, but not limited to vehicles, vessels, boats, airplanes, jet skis, all-terrain vehicles, RVs, personal property, and timeshare ownership, and any other evidence of unexplained wealth;

i. Items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the premises, including but not limited to canceled mail, deeds, leases, rental agreements, photographs and videos, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys;

j. Documents indicating travel in interstate and foreign commerce, to include airline tickets, notes and travel itineraries; airline schedules; bills; charge card receipts; hotel, motel, and car rental statements; correspondence with travel agencies and other travel related businesses; airline, rent a car, and hotel frequent flier or user cards and statements; passports and visas; telephone bills; photographs of foreign locations; and papers relating to domestic and international travel;

k. Safes and locked storage containers, and the contents thereof, which are otherwise described in this document;

l. Evidence of storage unit rental or access, including rental and payment records, keys and codes, pamphlets, contracts, contact information, directions, passwords or other documents relating to storage units;

m. Documents, records or information relating to the purchase, sale, tracking, delivery or distribution of postage or express mail consignment;

n. Documents, records or information relating to the transfer, purchase, sale or disposition of cryptocurrency;

n. Documents, records, or information relating to email accounts used in furtherance of these offenses;

o. Documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

p. Physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data;

q. Passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

r. Records or other items which are evidence of ownership or use of computer equipment found in the Target Residence, including, but not limited to, sales receipts, bills for internet access, handwritten notes and handwritten notes in computer manuals.

s. Cryptocurrency in any format, including but not limited to, wallets (hardware, digital and paper), public keys (addresses), private keys, and recovery seeds;

t. Latent prints and identifying material from items at the Target Residence.

2. **The items to be searched for, seized and secured are**:

a. Cellular telephones, tablets, iPads, and computers and other digital and electronic devices capable of storing data that constitutes evidence or the instrumentality of money laundering and narcotics trafficking.

**AGENTS ARE AUTHORIZED TO SEARCH FOR, SEIZE, AND SECURE, BUT NOT ANALYZE, DIGITAL DEVICES, INCLUDING CELL PHONES, TABLETS, IPADS, COMPUTERS AND ELECTRONIC STORAGE MEDIA AS DEFINED HEREIN. ANY SEARCH OR ANALYSIS OF SAID ITEMS MUST BE CONDUCTED PURSUANT TO A**

**SEPARATE SEARCH WARRANT OBTAINED FROM THE WESTERN DISTRICT OF WASHINGTON.**

3. During the execution of the search of the Target Residence described in Attachment A, law enforcement personnel are authorized to press the fingers, including thumbs, of ANDREW TONG, found at the Target Residence to the Touch ID sensor of the Apple brand devices, such as an iPhone or iPad, found at the Target Residence for the purpose of attempting to unlock the device via Touch ID as authorized by this warrant. Law enforcement are authorized to take steps to secure the unlocked Apple brand devices, including by changing the passwords of said devices.

4. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, DVDs, flash drives, USBs, thumb drives, and other magnetic or optical media.

# ATTACHMENT A

## (Target Residence to Be Searched)

The property to be searched is 14856 Southeast Spanish Bay Drive, Happy Valley, Oregon, further described as a single family house with brick and gray siding. This residence has a gray single and a gray double garage door facing the street and a wooden front door. The numbers 14856 are in rock above the archway in front of the door.

DISTRICT OF OREGON, ss: AFFIDAVIT OF JUSTIN HUSSEY

**Affidavit in Support of an Application Under Rule 41 for a Search Warrant**

I, Justin Hussey, being duly sworn, do hereby depose and state as follows:

## I. INTRODUCTION AND AGENT BACKGROUND

1. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

2. I am a Special Agent with the Department of Justice, Drug Enforcement Administration (DEA) and have been since July 2017. I am currently assigned to the DEA Portland District Office. As a Special Agent of the DEA, my duties and responsibilities have included conducting criminal investigations for possible violations of federal law, particularly those found in Title 18 and Title 21 of the United States Code. I have received specialized training from the DEA, to include a 20-week Basic Agent Training course in Quantico, Virginia. Prior to joining DEA, I worked as a Police Officer with the City of Hickory Police Department in Hickory, North Carolina, for approximately six years. Before that, I was employed as a Deputy Sheriff with the Burke County Sheriff's Office in Morganton, North Carolina, for approximately five and a half years.

3. Based upon my experience, training, and discussions with senior agents, I am familiar with the manner in which narcotic traffickers and money launderers conduct their business, including, but not limited to, their methods of importing and distributing controlled substances, their use of cellular telephone technology, computers, and the internet, and their use of numerical codes and coded and/or cryptic language, words, and references to conduct their

transactions. Further, I have conducted physical surveillance, electronic surveillance, and the execution of search warrants.

4. The facts in this affidavit come from my training, experience, and information obtained from other agents and witnesses.

## II. PURPOSE OF THIS AFFIDAVIT

5. I make this affidavit in support of an application for a warrant authorizing the search of the following residence, which is further described below and in Attachment A (attached hereto and incorporated by reference as if fully set forth herein), for evidence, fruits and instrumentalities, as further described in Attachments B (attached hereto and incorporated by reference as if fully set forth herein), of the crimes of *Conspiracy to Commit Money Laundering*, in violation of 18 U.S.C. §§ 1956, 1957, and 1956(h); *Money Laundering*, in violation of 18 U.S.C. § 1956; and *Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity*, in violation of 18 U.S.C. § 1957 (the "Subject Offenses"), as described herein:

a) **Target Residence:** 14856 Southeast Spanish Bay Drive, Happy Valley Oregon is believed to the residence of Andrew TONG, whom investigators believe is laundering the cash drug proceeds of Anthony PELAYO. The **Target Residence** is a single family house with brick and gray siding. The **Target Residence** has a gray single and a gray double garage door facing the street and a wooden front door. The numbers 14856 are in rock above the archway in front of the door.

6. For the **Target Residence**, authority to search extends to all parts of the property, including main structure, garage(s), storage structures, outbuildings, and curtilage, and all

vehicles, containers, compartments, or safes located on the property, whether locked or not where the items described in Attachment B (list of items to be seized) could be found.

## III. SOURCES OF INFORMATION

7. I am not the case agent on this investigation. I make this Affidavit based upon my training and experience investigating money laundering and drug trafficking and related criminal activity, as described above, and knowledge derived from information reported to me by experienced agents working on this investigation, including DEA SA Joseph Cheng. I believe those agents to be reliable, based in part on their use of the following sources during this investigation:

a. Physical surveillance conducted by the aforementioned agencies, and other law enforcement agencies, that has been reported to me directly or indirectly;

b. Confidential sources/informants;

c. Telephone toll records, pen register and trap and trace information, and subscriber information;

d. Records from the Washington State Department of Licensing, or the equivalent agency in other states;

e. Information obtained as a result of Court-authorized search warrants; and

f. Review of records obtained from financial institutions.

8. This Affidavit is intended to show only that there is probable cause for the requested warrant and does not set forth every fact known to me concerning these matters. I have set forth only the facts that I believe are essential to establish the necessary foundation for search warrants for the Target Residence.

9. In the following paragraphs, I describe communications between various individuals. Except where specifically indicated with quotation marks, the descriptions are summaries of the conversations and are not meant to reflect the specific words or language used.

## IV. SUMMARY OF INVESTIGATION

10. An ongoing investigation is being conducted by the Drug Enforcement Administration (DEA) into the importation of powdered fentanyl and its analogues by Bradley WOOLARD, and others, both known and unknown. Investigators believe that WOOLARD (and, possibly, others) ordered the fentanyl over the internet from China. Once WOOLARD and/or his coconspirators received the powdered fentanyl through the mail, WOOLARD caused the fentanyl to be pressed into fentanyl-laced counterfeit oxycodone pills, by Anthony PELAYO. Once pressed into pills, WOOLARD, PELAYO, Timothy MANTIE and others distributed these dangerous pills into the community.

11. In July and August 2018, investigators executed multiple federal search warrants at WOOLARD's residence, located at 9717 99th Avenue Northeast, Arlington, Washington (hereinafter the "WOOLARD Residence"). Pursuant to those search warrants, investigators seized approximately 10,000 light blue pills marked "M30" which tested positive for furanyl fentanyl, a fentanyl analogue. Investigators seized numerous items during the searches of the WOOLARD Residence and outbuildings, including 33 firearms (the majority of which were concealed in a hidden room in a shop on the property), thousands of rounds of ammunition, approximately $1.1 million in suspected drug proceeds concealed in various locations throughout the WOOLARD Residence and in the shop areas on the property, and cell phones, including an Apple iPhone. Investigators seized multiple documents from the WOOLARD Residence

referencing telephone number (360) 395-5222 and email: bradwoolard79@gmail.com as being used by WOOLARD.

12. Investigators searched the iPhone and iPad seized from the WOOLARD Residence pursuant to search warrants. Investigators learned this iPhone was assigned (360) 395-5222 and Apple ID bradwoolard@ymail.com. Two email accounts were synced with this iPhone, bradwoolard@ymail.com and bradwoolard79@gmail.com. Review of emails on this phone revealed email exchanges between WOOLARD, using bradwoolard79@gmail.com, and individuals who appeared to be based in China. In these emails, WOOLARD and the China-based individuals openly discussed WOOLARD attempting to obtain various chemical substances, including fentanyl and furanyl fentanyl, from China.

13. Investigators discovered that the iPad had a listed owner of "Brad's iPad" and an Apple ID of bradwoolard@ymail.com. In this iPad investigators located numerous messages between WOOLARD and PELAYO in which WOOLARD was providing PELAYO with a recipe on how to mix "active," which investigators believe to be fentanyl or a fentanyl analogue, to press into pills. Additionally, investigators identified a photograph sent to WOOLARD by PELAYO which appeared to depict a pill press.

14. Investigators subsequently conducted a search warrant at PELAYO's residence and obtained an additional search warrant for cell phones seized from PELAYO's person. During the search of those phones, investigators identified approximately 135,000 messages between PELAYO and Andrew TONG. In those messages, they discussed the laundering of PELAYO's drug proceeds, which included the structured deposits of cash into PELAYO's accounts, as well as PELAYO's purchase of an RV, which was purchased in TONG's name.

15. In light of the investigation to date, to include the seizures from the WOOLARD and PELAYO residences, the known communications between PELAYO and TONG, and the records discussed herein, there is probable cause that evidence, fruits, and instrumentalities of TONG's and PELAYO's money laundering activities will be found at the **Target Residence**.

16. On June 12, 2019, a federal grand jury in the Western District of Washington returned a Superseding Indictment charging WOOLARD, Anthony PELAYO, Shawna BRUNS, Robert TABARES, Keith STRAND and Adrian BERGSTROM in *United States v. Woolard, et al.*, CR18-217RSM, with *Conspiracy to Distribute Controlled Substances*, in violation of 21 U.S.C. §§ 841(a)(1), 841(b)(1)(A) and 846 (Count 1), *Money Laundering Conspiracy*, in violation of 18 U.S.C. §§ 1956(a)(2)(A) (Count 13), and additional substantive drug trafficking and substantive counts. WOOLARD was also charged with *Felon in Possession of Firearms*, and *Unlawful User of Controlled Substances in Possession of Firearms*, in violation of 18 U.S.C. § 922(g)(1), and *Possession of Firearms in Furtherance of a Drug Trafficking Offense*, in violation of 18 U.S.C. § 924(c). PELAYO was also charged with two counts of *Possession of Firearms in Furtherance of a Drug Trafficking Offense*, in violation of 18 U.S.C. § 924(c). PELAYO, BRUNS, TABARES and STRAND were not charged in the Indictment previously returned by the Grand Jury.

17. On June 12, 2019, BRUNS, TABARES, STRAND and BERGSTROM were arrested, and the Superseding Indictment was unsealed. An arrest warrant was issued for PELAYO on June 12, 2019, however, PELAYO was not arrested until June 21, 2019. Following detention hearings for TABARES, STRAND and BERGSTROM on June 18, 2019,

the Court released all three individuals on pretrial supervision. BRUNS and PELAYO are currently detained pending trial.

## V. PROBABLE CAUSE

18. As discussed herein, DEA is investigating fentanyl trafficking and related offenses in the Western District of Washington and elsewhere, by Bradley WOOLARD and his criminal associates. The investigation is ongoing. Based on my training and experience, and information relayed to me by other law enforcement personnel, I know that fentanyl is a Schedule II narcotic and a highly dangerous drug. Fentanyl is a synthetic opioid that is 50 times more toxic than heroin. In its purest form, fentanyl is a white powder or in grains similar in size to table salt. For most people, two to three milligrams of fentanyl is capable of inducing respiratory depression, arrest and possibly death. Two to three milligrams of fentanyl is comparable in size to five to seven individual grains of table salt. Additionally, counterfeit Percocet pills have been associated with multiple overdose deaths in Skagit and Snohomish Counties in 2018 and 2019, and fentanyl has been linked to multiple overdoses in Snohomish County, Washington.

### A. Execution of Multiple Search Warrants of the WOOLARD Residence in July and August 2018

19. On July 28, 2018, the Honorable Mary Alice Theiler signed a search warrant authorizing the search of 9717 99th Avenue Northeast, Arlington, Washington (the WOOLARD Residence), *i.e.*, the residence of WOOLARD, Shawna Marie Bruns (WOOLARD's wife), and their minor children. During the execution of the search warrant that day, investigators found approximately 10,000 of the counterfeit Percocet pills located in the office of the main residence. In this office, there were numerous documents with the name Bradley WOOLARD.

Additionally seized from the office was a small container of blue dye, which investigators suspect could have been used by WOOLARD in the process of pressing white fentanyl powder and binding materials into counterfeit M30 pills. These pills were submitted to the DEA laboratory for testing and the laboratory counted 12,389 pills and indicated that they tested positive for furanyl fentanyl.

20. Investigators also found approximately $400,000 in cash located in two safes, one in the office and one in the master bedroom closet. Items of dominion and control with WOOLARD's name were found in the office and master bedroom.

21. During the July 28 search of the WOOLARD Residence, investigators seized two shipping labels from the trash in the office. One shipping label had the sender and recipient removed but described the contents as "Lab supplies" with a weight of 0.1 kilograms, a value of $5.00 and goods' origin of "CN". A second shipping label was largely intact and also listed the contents as "Lab supplies" with the same weight, value and goods' origin. This shipping label showed "Danette Skelton" and "32326 Mountain Loop Hyway, Granite Falls WA USA 98252" as the "ship to" information and the "from" information listed "Wuzong Hui" and "China 61 Jianning Road No. 3 Building 1502 Room GulouQu, Nanjing Jiangsu 210000." Additionally the shipping labels listed tracking number LS508043116CN. According to the USPS website, this package was delivered to the Granite Falls address on January 29, 2018.

22. On August 16, 2018, the computer and other digital devices present in the WOOLARD Residence, including an Apple iPhone and iPad were seized pursuant to a federal search warrant that had been issued by U.S. Magistrate Judge Paula L. McCandlis on August 15, 2018. The search of WOOLARD's iPad is discussed below.

**B. Two Packages of Fentanyl Shipped from China Intercepted by Law Enforcement**

23. As discussed above, the shipping labels found in the WOOLARD Residence listed the "from" information as "Wuzong Hui" and "China 61 Jianning Road No. 3 Building 1502 Room GulouQu, Nanjing Jiangsu 210000." Investigators identified two additional parcels that were en route to Western Washington from the same shipper as listed on packaging materials found in the WOOLARD Residence. Both parcels were intercepted. On August 2, 2018, investigators obtained federal search warrants for the two additional parcels, one of which was addressed to Sadie BATES at 12118 Hwy 99 #J 402, Everett, Washington, tracking number LY460463148CN, and one of which was addressed to Adrian BERGSTROM at 200 East Maple St Apt 507, Bellingham USA US 98225, tracking number LY466322829CN.

24. The parcels were searched pursuant to the warrant. The contents of both parcels was submitted to the DEA laboratory for testing. According to the DEA laboratory, the contents of both parcels tested positive for Furanyl Fentanyl and the contents weighed approximately 99.4 grams and 99.6 grams.

25. During this investigation, investigators searched WOOLARD's email messages pursuant to federal search warrants. The messages indicate that WOOLARD was communicating with sources of supply in China to obtain fentanyl, fentanyl analogues and other controlled substances since approximately February of 2016. The above referenced parcels were amongst those that WOOLARD obtained from his Chinese sources of supply.

**C. Search of iPad seized from WOOLARD's residence**

26. During search of WOOLARD's residence, investigators seized an iPad. The search warrant signed by US Magistrate Judge Paula L. McCandlis on October 5, 2018,

authorized the search of this device. The "Owner Name" is listed as "Brad's iPad" and the associated Apple ID is bradwoolard@ymail.com. As discussed above, this is WOOLARD's known Apple ID. Investigators located numerous photos stored in this device that depict WOOLARD and BRUNS.

27. Investigators reviewed iMessages between bradwoolard@ymail.com and 1-425-404-1227, which is saved under the contact name "Tonny." Based on the investigation to date, investigators believe this phone to be used by Anthony PELAYO. On January 29, 2017 WOOLARD and PELAYO exchanged the following messages:

WOOLARD: "U should run enuf to get by til I'm back before u move it. Might need my adjustments after the ride."

PELAYO: "Ya that is my plan I'm gonna run that whole bucket at least then c where I'm at."

PELAYO: "Tim never hit me up dude said he will swap that 30 tomo"

WOOLARD: "Might be a day or two. U know how it goes"

WOOLARD: "But thank you."

WOOLARD: "This will be a good thing for us. Safe to only I know where and I'm as solid as a rock."

WOOLARD: "I just made a offer on a beach house. Our family's can have fun this summer and for a long time."

PELAYO: "O ya I'm gonna save every penny to ya this is gonna b hella good I'm gonna b working this week on cleaning some shit out and all that good stuff"

WOOLARD: "Good deal. Please toss the old presses out for me"

WOOLARD: "Keith will help. I'll send his #"

PELAYO: "Ok would you mind if I take them apart so I could just put them in different bags"

WOOLARD: "Not at all use my tools whatever u need"

PELAYO: "Ok cool that will be lighter when I toss it."

28. Based on the ongoing conversation, the ongoing investigation, and my training and experience I believe, in this conversation, that PELAYO and WOOLARD are discussing PELAYO pressing a large quantity of pills before WOOLARD left town and that WOOLARD asked PELAYO to dispose of some old pill presses[1] for WOOLARD.

29. The following exchange between WOOLARD and PELAYO, using the 425-404-1227, occurred on February 7, 2017:

WOOLARD: "Tim said the things were bad. I'll call him in a he to see how."

WOOLARD: "A hr"

WOOLARD: "U will have to make adjustments"

PELAYO: "Ok just let me kno cuz those r the ones me and u made"

WOOLARD: "Really?? They should be fine"

PELAYO: "Ya, I haven't gave him any yet the last ones he got were from u"

WOOLARD: "I guess the strength is down a bit and not quite hard enuf. Both will be fixed by increasing the weight. Please weigh them and if you can break them with your fingers they are to soft. Moving the machine did this I'm sure."

[1] A pill press (or encapsulating machine) and its associated equipment are used to convert powder drugs (e.g., powdered fentanyl) to pill form (e.g., fentanyl-laced counterfeit M30 pills).

PELAYO: "I was about to over there to work what should I do"

PELAYO: "Ya I was weighing the ones I made made sure they're were 128 right"

WOOLARD: "We might have to add a lil active to it. We will have to grind and repress when I get back but for now we just fix and make more. They should weigh I'll know more later just hang tight for now."

WOOLARD: "Pull the dry pads out that might be affecting it"

WOOLARD: "Fuck"

PELAYO: "Ok"

PELAYO: "I moved almost 2k so far and no one has called me I wonder why they calling him that's weird"

WOOLARD: "I'll do some math and u can add like .02 mg to each on before next press. They have bigger tolerances."

WOOLARD: "He has fiends"

WOOLARD: "I'll hit u back later"

PELAYO: "Ok should I go take those pads out real quick"

PELAYO: "Or just wait for ur call"

WOOLARD: "I'm doing some math. Give me a min"

WOOLARD: "Ok weigh out 1560g of mix. Add 2.5g of active that has been ground. Mix super good. That will make close to 12000 for his next batch. Make them. 130 ea but same size. Should fix it."

30. In the messages described above, investigators believe that PELAYO told WOOLARD that their customer "Tim" (believed to be MANTIE) complained about the potency

of the pills. Investigators believe that the term "active," as used by WOOLARD, is a reference to the active ingredient in the pills, believed to be fentanyl or a fentanyl analogue. Investigators believe that WOOLARD and PELAYO discussed how to increase the potency of the pills that PELAYO was pressing on WOOLARD's behalf in response's to MANTIE's complaint about potency. The message exchange concluded with WOOLARD providing PELAYO with an updated "recipe" for the pills. Additionally, when PELAYO said, "I moved almost 2k so far and no one has called me," investigators believe that PELAYO told WOOLARD that PELAYO has distributed 2,000 pills himself and they did not complain about the quality.

31. On February 8, 2017, PELAYO sent the photograph below to WOOLARD followed by a message that said "call me."

32. Investigators conducted an internet search for pill presses with a similar appearance. Investigators identified a RTP9 Rotary Tablet Press, sold by LFA Tablet Press that appeared consistent in appearance to the above photograph. According to the LFA website, this pill press weighs 260 kg or 485 pounds. Investigators have obtained court authorization for search warrants on approximately 10 separate locations through the course of this investigation and have been unable to locate the pill press depicted in the above photograph or any other pill presses. Based on the messages between PELAYO and WOOLARD, investigators believe that PELAYO had access to and knew the location of the pill press utilized by WOOLARD and PELAYO to press fentanyl laced pills.

33. On March 27, 2017, WOOLARD sent to PELAYO, "R u up? I'm going to my cabin and was going to drop that 5000 on way." PELAYO replied, "I gotta get em finished I thought U where gonna give me a day notice I will have it ready for u in a few hrs tho" and "I'm only short a few k." On March 30, 2017, PELAYO sent "Hey I guess Noi client canceled do u wanna go back out there tomo and mess with the machine" and WOOLARD replied "yes." PELAYO then sent, "Koo I'll come by after the gym again" and WOOLARD replied "k" and "I got that pkg to."

**D. Execution of Search Warrants at PELAYO's Residences**

34. On May 29, 2019, US Magistrate Judge Paula L. McCandlis signed search warrants authorizing the search of two of PELAYO's residences and TABARES's residence. On May 30, 2019, investigators executed these search warrants as described below.

35. On May 30, 2019, investigators observed PELAYO depart his residence (located at 3423 68th Drive, Marysville, Washington) and drive to Team Fitness in Lake Stevens,

Washington. Uniformed officers detained PELAYO at Team Fitness, pending the execution of the search warrant at his residence. During a pat down of PELAYO's person, investigators located a cell phone. Investigators advised PELAYO of his *Miranda* Rights, and PELAYO agreed to speak to investigators. PELAYO told investigators that there was a firearm in the center console of his vehicle and signed consent for investigators to search his vehicle. Found in PELAYO's vehicle was a rose gold Apple iPhone.

36. Investigators subsequently made entry to PELAYO's residence (3423 68th Drive Northeast, Marysville, Washington) pursuant to the search warrant. During the search of the residence, investigators found in the kitchen of the residence a pill bottle with the label removed, which contained approximately 25 pills marked "M30." The DEA Western Laboratory subsequently determined that these pills contained oxycodone, a Schedule II narcotic. Also found in the same drawer was approximately $19,461 in US Currency and a box of Narcan nasal spray. Narcan is a trade name for naloxone and naloxone is a drug used to block or reverse the effects of opioid drugs (fentanyl is an opioid). Based on my training and experience I know that naloxone is frequently used to treat opioid overdose. Located approximately 10 feet away, also in the kitchen, on top of the refrigerator was a Glock 19 handgun with a loaded magazine in the weapon but no round in the chamber.

37. In a child's bedroom, investigators located a bag which contained approximately $100,000. Across the hallway from the child's bedroom was the master bedroom. A safe was located in the master bedroom and PELAYO unlocked the safe for investigators. Located within the safe was a loaded revolver and another handgun. This handgun had also had a loaded magazine in the weapon and no round in the chamber.

38. Found in the garage of PELAYO's residence were two digital scales, a large industrial mixer, approximately 3 feet tall, and a gun safe which contained nine firearms. Although the mixer appeared to be unused, PELAYO told investigators that the mixer was used to make sauces.

39. In total investigators seized approximately $129,201 in US Currency, 13 firearms, 25 oxycodone pills, five vehicles, including a Harley Davidson motorcycle, and other evidence of drug trafficking from PELAYO's residence on 68th Drive Northeast.

40. Investigators also searched PELAYO's property located at18222 Russian Road, Arlington, Washington.[2] At this location, investigators seized documents of dominion and control and two vehicles, *i.e.*, an RV and a John Deere tractor. As further described below, investigators believe PELAYO provided cash drug proceeds to TONG, so that TONG could put the RV in TONG's name, in an attempt to conceal that PELAYO was the true owner of the RV. Investigators did not locate any drugs, drug proceeds, drug paraphernalia or firearms from the Russian Road residence.

**E. Searches of PELAYO's Cell Phones and Financial Records Reveal TONG's Laundering of PELAYO's Cash Drug Proceeds**

41. Investigators obtained search warrants to search the cell phones seized from PELAYO and subsequently searched those devices. Investigators identified approximately 135,000 messages between PELAYO and 503-806-2434. This phone number was saved in

[2] According to Washington DOL, PELAYO updated his address to the Russian Road property on April 1, 2019, and has several vehicles that list the Russian Road property as the location address. According to the Snohomish County Assessor's website, "LB Trust" purchased the Russian Road property in 2011. The listed address on the Snohomish County Assessor's website for LB Trust is 3423 68th Drive Northeast, Marysville, Washington.

PELAYO's phone as "Andrew Portland." According to AT&T records, the financial liable party for 503-806-2434 is Naren Soutavong at 13268 Southwest Shore Drive, Tigard, Oregon and the user information is listed as Andrew TONG at 13268 Southwest Shore Drive, Tigard, Oregon. The first text message on PELAYO's phone with TONG is dated November 17, 2016.

42. In text messages between PELAYO and TONG, the two discuss PELAYO's lucrative drug trafficking. PELAYO and TONG also discuss their laundering of PELAYO's drug proceeds by purchasing the RV (discussed above) and putting it in TONG's name; by TONG structuring cash deposits into PELAYO's bank accounts; TONG's purchase of a $100,000 cashier's check, which was deposited into PELAYO's bank account; and numerous wire transfers of funds by TONG into PELAYO's bank accounts. Based upon review of text messages exchanged between PELAYO and TONG, and the financial records obtained thus far, it appears that TONG knowingly laundered over $300,000 of PELAYO's cash drug proceeds. Additionally, it further appears that while PELAYO was a fugitive, PELAYO transferred $200,000 to TONG. Investigators believe that these transfers by PELAYO to TONG represent additional attempts by PELAYO to conceal his drug proceeds from law enforcement and avoid seizure thereof. I discuss some, but not all, of the messages between PELAYO and TONG and pertinent financial records below.

43. On December 15, 2016, PELAYO sent to TONG, "Those dummies made my xmas today lol." TONG responded, "U?," "Lol," and "How much." PELAYO responded "6800." Later in the conversation, PELAYO said, "I had to pull the heat out on this lil nigga tho just to show him he better not try nothing stupid lol" and "straight dummies lol." The conversation continue into the following day when TONG said, "Damn how many was it" and

PELAYO responded "16k worth lol." TONG then asked, "I know but how many dummies lol." PELAYO responded, "1k." Later in the same conversation, PELAYO told TONG, "Na the dummies get u fucked up its just a different active ingredient," "they actually stronger," and "but don't last as long and u can't smoke it." Based on my training and experience, I believe that PELAYO and TONG are using the term "dummies" as code for the counterfeit oxycodone pills, which contained fentanyl, which PELAYO and WOOLARD were pressing and distributing. Additionally, investigators believe that in this conversation, PELAYO told TONG that he sold 1,000 counterfeit oxycodone pills for $16,000 and PELAYO made $6,800 during the transaction.

44. On January 5, 2017, PELAYO sent to TONG, "I need to get my jugs up the plug putting me on at the end of the month I literally can make whatever I want if I can move enough of em" and "this fool makes like 200k a month." Based upon my training and experience, I know that the term "plug" is often used to refer to a source of supply for drugs. These messages are consistent with the messages discussed above, found in WOOLARD's iPad from January and February 2017 when WOOLARD and PELAYO are discussing PELAYO pressing pills while WOOLARD is out of town.

45. According to banking records for some of PELAYO's accounts, on February 7, 2017, PELAYO opened JPMorgan Chase checking and savings accounts in the name of Pelayo & Sons LLC, *****3088 (checking) and ******6703. Later, on June 6, 2018, PELAYO opened Chase accounts ******5330 and *****3576 (checking). Review of bank records for the time period of 2018 through July 29, 2019 shows that deposits to PELAYO's checking accounts totaled approximately $477,953.28. TONG's role relating to some of these deposits is discussed below.

46. On February 25, 2017, TONG sent, "damn I might have a client" and "how many milligrams those dummies?" PELAYO responded, "30." TONG then asked, "how much for hundred" and PELAYO replied, "1500" and "you should be able to sell it from anywhere from 2 to 2200." TONG and PELAYO continue to discuss TONG's possible customer and TONG obtaining a sample until TONG asked, "What's the real name for it" and "like what's it mostly of." PELAYO responded, "just tell em they percs."

47. In the above text exchange, I believe that TONG asked PELAYO to clarify the dosage of pills that PELAYO distributed, and PELAYO told him "30." This is consistent with the fentanyl-laced counterfeit "M30" pills distributed by PELAYO and WOOLARD. Also, the price quoted by PELAYO -- $1,500 for one hundred of these pills – is consistent with the wholesale prices for these pills. When PELAYO told TONG, "you should be able to sell it form anywhere from 2 to 2200," I believe PELAYO meant that TONG would be able to sell those pills for $2,000 to $2,200, which would yield TONG profit in the amount of $500-$700. Additionally, it appears that PELAYO told TONG to tell his potential customer that the pills were "percs," a term which commonly refers to Percocets (i.e., real pills, as opposed to counterfeit pills).

48. On May 12, 2017, TONG wrote, "You need to pay someone to launder your money to put it on paper for u," "Idk where," "You need to spread it out too to make it legit." PELAYO texted, "I got like 14k on pap" and TONG replied, "yeah you gonna need way more," "Before u file ur taxes," and "that way you can use it." Similarly, in messages on March 5, 2018, TONG and PELAYO discussed going to college, then PELAYO wrote to TONG, "I just wanna learn how to launder money" to which TONG, "shit u need someone to poen shit for u

under their name" and "thought u was gonna open up those coffee shops." PELAYO later wrote, "It's hard for me to commit to something cuz I look at the money start a business and make 100-200 a year I can make more than that in a month." Based on these text messages, and the other evidence discussed herein, it appears that PELAYO and TONG are very well aware of the need for PELAYO to launder his drug proceeds, and the purpose of their bulk cash transfers, vehicle purchases and wire transfers.

49. According to the Washington State Department of Revenue's public website, Anthony PELAYO opened a sole proprietorship in the name of Tony's Automotive Upholster (UBI 604 104 314) on March 20, 2017. (A screenshot located during the execution of search warrants show the actual online filing date was March 14, 2017.) PELAYO and TONG discussed the formation of this business in the days before PELAYO did the online filing date for it. PELAYO texted, "I'm about to file for m business license." TONG replied, "Online?" PELAYO responded, "Yeah." TONG responded, "They gonna knock on ur door" and "Lol." PELAYO responded, "Na hell no I've been doin it for 7 years but imma start claiming more money so I wanna get a business account" and added, "So I can get a business loan."

50. In addition to the messages where PELAYO told TONG about his drug trafficking activities and how much money PELAYO was making, PELAYO described vehicles which he purchased, including a Harley Davidson motorcycle and John Deere tractor. Both of these vehicles were seized from PELAYO's residences during the above described search warrants and were registered in a third party's name (a suspected straw owner).

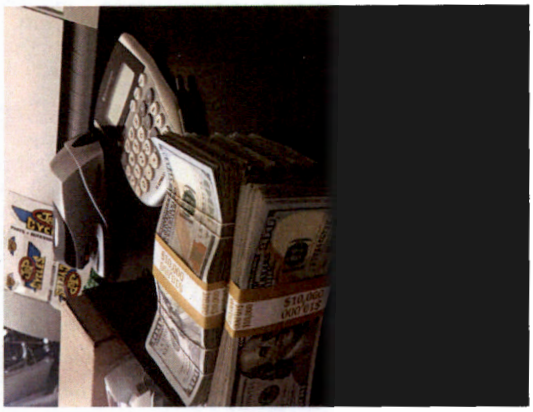
51. Beginning in 2017, and continuing into early 2018, PELAYO and TONG discuss having TONG purchase an RV, using cash provided by PELAYO, in an attempt to conceal that the true owner of the RV was PELAYO. I discuss some, but not all, of the texts herein.

52. For example, on February 8, 2018, PELAYO and TONG discuss PELAYO purchasing the RV in Oregon to avoid sales taxes and PELAYO said, "ya I'll put under Noi's name" and "or someone down there." TONG responded, "Or put it in mine. I just don't know how to drive it."

53. On February 17, 2018, PELAYO texted TONG that, "ya it's a sketchy life bro u paranoid all the time specially when u making crazy money" and "that's just sitting in my kitchen drawer." The latter message was accompanied by the following photograph:

54. Later that same day, PELAYO texted TONG that, "Time to get to work counting I had to super flue my money counter shit broke lol," "I've had it for almost 10 years," and "shits counted millions already" and sent TONG a photo of a money counter. Later PELAYO texted

TONG that, "gotta get this rv money ready." As this conversation continued, PELAYO sent the following two photos to TONG.



55. PELAYO also sent TONG a video. This video depicted multiple bundles of US currency banded together, and PELAYO told TONG, "and that's 500k."

56. The messages confirm on March 18, 2018, TONG purchased an RV on PELAYO's behalf with cash brought to Oregon by PELAYO. Specifically, on March 18, 2018, TONG said, "U bout to buy a rv" and PELAYO responded, "no u r." Also, TONG said, "chump change after I saw u drop 103k on those fools." Additionally, PELAYO said, "do they know I paid in cash." This RV was seized from PELAYO's residence located on Russian Road in Arlington, during the search warrant discussed above and is indeed registered to Andrew TONG, at 13268 Southwest Shore Drive, Tigard, Oregon.

57. Investigators have interviewed employees at Camping World RV in Wood Village Oregon regarding the purchase of this RV. The employees recalled the transaction because of its unusually large amount of US currency. An employee involved in the transaction was shown photographs of PELAYO and TONG and stated that both were similar in appearance to the individuals who bought the RV. The employees stated that the purchaser, TONG, stated

that he was an "Instagrammer" and that he got the money for the RV from his "Instagram" activity.

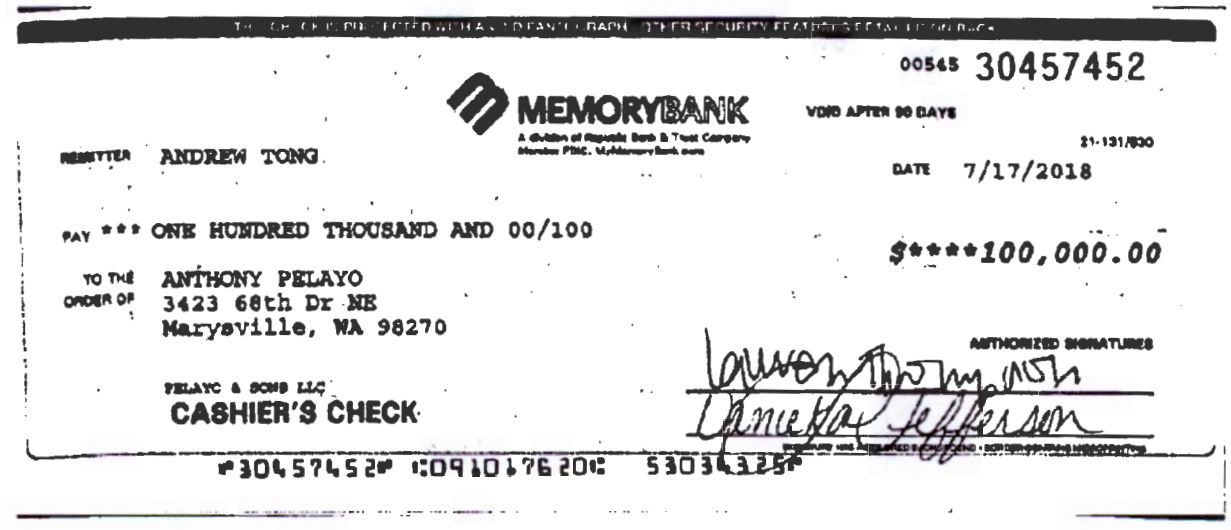
58. On July 16, 2018, PELAYO asked TONG, "U still wanna do that 100k shit?" and TONG responded, "Whenever u want me to call them and send you a cashier check." PELAYO responded, "Lol ok imam send the loot with Noi II'm sure u will c here at grandpas." Later TONG said, "What should I tell them to put in the memo?" and "Pelayo investments?" PELAYO replied, "Make it out to pelayo & sons llc." And TONG replied, "But with your name?" "or just that." PELAYO responded, "you can put my name on it to." The following day PELAYO sent, "hey so you want all 100's right." Later in the same conversation, PELAYO sent TONG the following photo and "U sure 20's."

59. On the same day, TONG asked "U got more to clean?" and PELAYO responded "Ya but we can do it later."

60. On July 19, 2018, TONG and PELAYO text about the cashier's check. TONG wrote, "I've never seen a check that big before" and "Nor have I seen soooo many twenties lol." PELAYO replied, "U give me a .5 ounce check I give u 30lbs in 20's lol." I believe these texts reflect that PELAYO provided the cash (30 pounds of $20 bills) to TONG to purchase a $100,000 cashier's check.

61. In the course of these discussions, TONG also texted PELAYO, "give Noi the heat" and "in case she needs to pistol whip these fools." (Noi is PELAYO's wife/significant other.) PELAYO responded, "Lol."

62. Consistent with the above text exchange, the following is a copy of a $100,000 cashier's check deposited into PELAYO's Chase bank account on July 19, 2018. The check indicates that the remitter (i.e., the individual who purchased the cashier's check) was Andrew TONG:


00545 30457452

MEMORYBANK

VOID AFTER 90 DAYS

REMITTER ANDREW TONG

21-131/830

DATE 7/17/2018

PAY *** ONE HUNDRED THOUSAND AND 00/100

$*****100,000.00

TO THE ORDER OF ANTHONY PELAYO
3423 68th Dr NE
Marysville, WA 98270

AUTHORIZED SIGNATURES

PELAYO & SONS LLC

CASHIER'S CHECK

⑈30457452⑈ ⑆091018762⑆ 530343325⑈

63. On October 17, 2018, TONG sent the following photo to PELAYO and said, "how do u want this," "I told u I got hella bills," and "want me to slowly put it into your

account?" Counting the money bands in the image below, there appears to be $90,000 in US currency.

64. PELAYO responded, "faster the better really" and TONG said, "well yeah but I don't wanna slam 10k a day," "that's irs," "I was thinking 8k a day" and "into you business account." PELAYO then sent a photograph which contained his bank account number and routing number and "Pelayo & sons llc." In these texts, I believe that PELAYO told TONG to make the deposits as quickly as possible. TONG cautioned, however, that he did not want to deposit a large quantity in one day due to the "IRS." I believe that TONG wanted to avoid the filing of a currency transaction report (CTR), which banks are required to file for cash transactions (deposits or withdrawals) of more than $10,000 in cash.

65. The above texts messages are consistent with structured cash deposits made into PELAYO's bank accounts. According to the bank records, $110,480 of the total deposits consisted of cash. The timing of the above discussion and the following deposits are consistent.

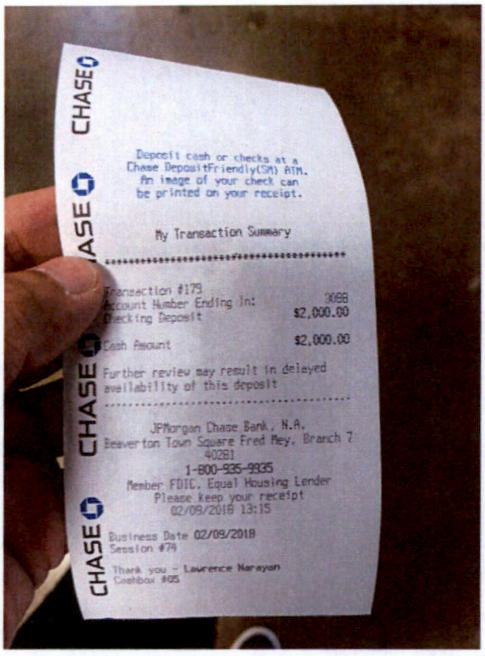
| Clear Date | Statement Description | Bank Item Description | Deposit |
|---|---|---|---|
| 10/23/2018 | Deposit | Cash In | $8,000.00 |
| 10/25/2018 | Deposit | Cash In | $8,000.00 |
| 10/26/2018 | Deposit | Cash In | $8,000.00 |
| 10/29/2018 | Deposit | Cash In | $8,000.00 |
| 10/31/2018 | Deposit | Cash In | $8,000.00 |
| | | | **$40,000.00** |

66. In addition, the bank records show that TONG wired an additional $134,880.00 into PELAYO's checking accounts:

| Clear Date | Statement Description | Deposit |
|---|---|---|
| 11/29/2018 | Fedwire Credit; The Bank of New York Mellon; Andrew Tong | $20,000.00 |
| 12/17/2018 | Fedwire Credit; The Bank of New York Mellon; Andrew Tong | $20,000.00 |
| 1/10/2019 | Fedwire Credit; The Bank of New York Mellon; Andrew Tong | $20,000.00 |
| 1/24/2019 | Fedwire Credit; The Bank of New York Mellon; Andrew Tong | $14,880.00 |
| 2/14/2019 | Fedwire Credit; The Bank of New York Mellon; Andrew Tong | $20,000.00 |
| 5/13/2019 | Fedwire Credit; The Bank of New York Mellon; Andrew Tong | $40,000.00 |
| | Total | $134,880.00 |

67. In addition, TONG sent PELAYO a receipt for a cash deposit made at Chase Bank. These receipts correspond to cash deposits made to PELAYO's accounts. For example,

on February 9, 2018, $2,000 in cash was deposited to PELAYO's checking account. Texts show that this same date, TONG sent PELAYO an image of a receipt for a $2,000 cash deposit into an account ending in –3088, the same as PELAYO's account:



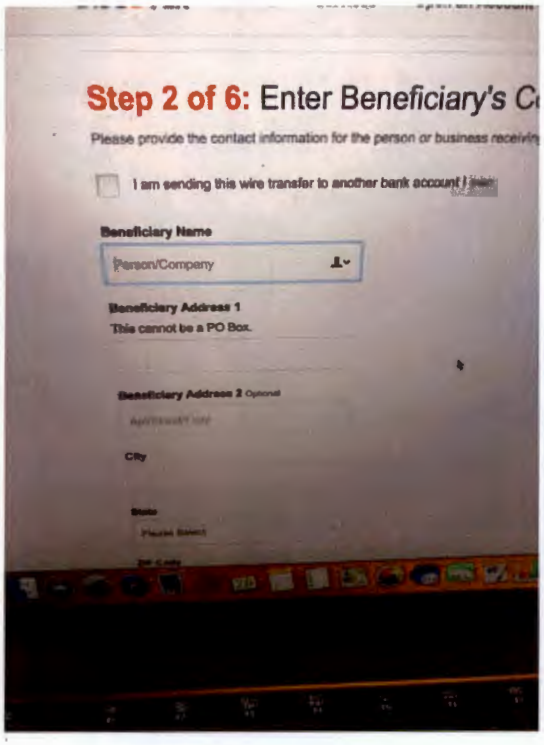

68. In addition to the cash deposits, on at least one occasion TONG stated that he put money into Bitcoin for PELAYO. On February 16, 2018, TONG texted, "I put 3k in bitcoin for u cause u wanted to trade lol."

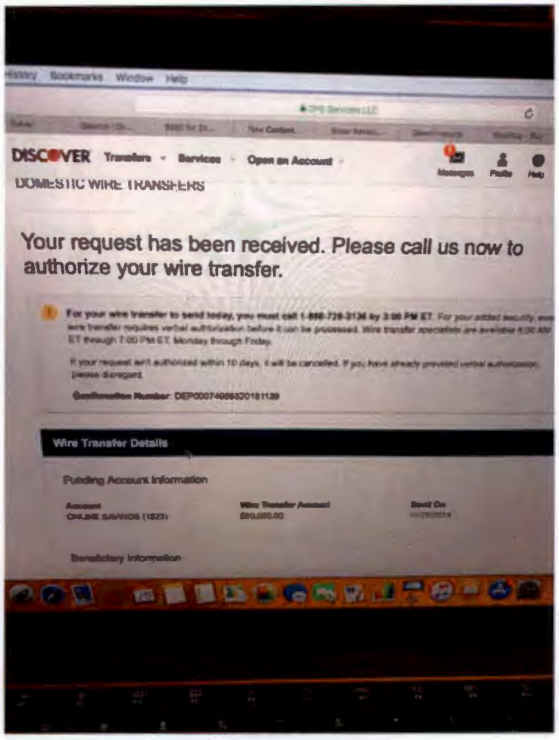
69. In early and middle 2019, TONG and PELAYO exchanged multiple messages where it appears that TONG is purchasing a new house. Specifically in on March 10, 2019, TONG sent a Zillow link to a house at 14856 Southeast Spanish Bay Drive, Happy Valley Oregon (**Target Residence**) and on March 11, 2019, TONG indicated that he put an offer in on the house. Subsequent messages indicated that TONG did indeed purchase the house and moved into it. On May 13, 2019, TONG asked, "Pelayo & sons llc?," "just sent," "40" and "you should get it by 5pm" and PELAYO acknowledged. Based on these text messages,

investigators believe TONG and PELAYO's money laundering activities continued after TONG moved into his new residence. As discussed above, on May 30, 2019, law enforcement contacted PELAYO and searched his properties on 68th and on Russian Road. On June 12, 2019, the Superseding Indictment was unsealed. Investigators attempted to locate PELAYO at his residence that day but were unsuccessful. On June 17, 2019, investigators interviewed PELAYO's wife and mother in an attempt to locate PELAYO. Based on statements made by both PELAYO's wife and mother, investigators believe that PELAYO already knew that there was a warrant for his arrest and that investigators were looking for him. As noted above, it was not until June 21, 2019, that PELAYO was arrested.

70. PELAYO's bank records show that on both June 17, 2019, and on June 18, 2019, PELAYO sent $100,000 wires to TONG, with the memo, "return investment property money." Based on these bank records and statements, investigators believe that PELAYO was attempting to hide his assets prior to his arrest, and, further, that PELAYO entrusted $200,000 of his drug proceeds with TONG.

71. TONG used a computer in furtherance of the money laundering conspiracy. For example, on November 28, 2018, TONG sent PELAYO photographs of a computer he was using to send wire transfers:




72. Review of CTRs show that TONG frequently gambles at casinos. From July 3, 2019, through September 18, 2019, CTRs were filed by four different casinos for TONG. Per these CTRs, TONG's total cash-in at these casinos totaled $700,329.00, and his cash-out totaled $682,130.

73. As noted above, on at least one occasion TONG stated that he put money into Bitcoin for PELAYO. That is, on February 16, 2018, TONG texted, "I put 3k in bitcoin for u cause u wanted to trade lol." This is only one example wherein targets of this investigation have discussed their use of Bitcoin.

74. During this investigators have obtained multiple search warrants in this investigation, to include warrants of WOOLARD's iPad, other digital devices, email addresses and cloud accounts. During these searches, investigators have located messages between

subjects of this investigation which discuss the obtaining and using of Bitcoin to further their drug trafficking activities, to include payment to WOOLARD's Chinese sources of supply for fentanyl. For example, in July 2018, PELAYO and WOOLARD discussed using Bitcoin to pay for purchase of fentanyl. In particular, PELAYO sent "Did she give u any tracking info" and WOOLARD replied, "Not yet I can't get ahold of her. She said they were having a huge storm two days ago and would ship when it passes." PELAYO said, "Ok people asking when they should expect it they want that money lol." WOOLARD replied, "Yes for sure. U will know the minute I do. What up w the btcn did I get there?"

75. Based on my training and experience, and discussions with other experienced agents, I know that 'BTC' is common shorthand for 'Bitcoin.' During this investigation, email messages between WOOLARD and one of his sources of supply in China, referred to as "Mary," indicated that WOOLARD was ordering fentanyl or fentanyl analogues from "Mary" in China. Additionally, investigators know from this investigation that WOOLARD caused Bitcoin to be sent to "Mary" as payment for fentanyl. Thus, in these messages investigators believe that PELAYO was asking when the fentanyl ordered by WOOLARD would arrive. The conversation continued, with PELAYO writing, "Ya dude can do it I'm gonna start doin sending this week." WOOLARD replied, "So u didn't send any?? I sent code." PELAYO responded "I haven't yet cuz the dude was out of town for the 4th" A few messages later, PELAYO said, "It's gonna be a few payments he can only do 15k at a time." WOOLARD said "Ok" and "I'll wait till I hear back." Investigators believe that PELAYO and WOOLARD are discussing obtaining Bitcoin from a third party to be used to pay for fentanyl from WOOLARD's source of supply in China.

**G. Records Checks for the Target Residence**

76. According to the Clackamas County tax assessor's website, the **Target Residence** was purchased by Andrew TONG on April 5, 2019 with a recording date of May 9, 2019.

77. According to Portland General Electric Company, the current customer of record for the **Target Residence** is Andrew TONG, the listed phone number is 403-806-2434 and the move in date is listed as May 10, 2019. This is the same number that TONG was using to communicate with PELAYO in the messages discussed above.

78. On October 16, 2019, investigators conducted surveillance at the **Target Residence**. Parked in the driveway was a white BMW bearing Oregon license plate TB15345. This vehicle is registered to Andrew TONG at 13268 Southwest Shore Drive, Tigard, Oregon.

## VI. KNOWLEDGE BASED ON TRAINING AND EXPERIENCE

79. Based on my training and experience, and my discussions with other experienced officers and agents involved in drug and money laundering investigations, I know the following:

a. Money launderers often have banking records to include but not limited to, deposit or withdrawal slips, bank statements, checks, or money orders. Some of these banking records may not be in their own name. Money launderers often have several accounts documented in some form, or instructions detailing how to handle each respective account. For example, they may have a list of accounts belonging to several different people with instructions for how much to deposit or withdraw from each and often maintain this information for long periods of time in their residences or safe deposit boxes.

b. Money launderers often have records or evidence related to how the proceeds were spent or concealed and often maintain this information for long periods of time in

their residences or safe deposit boxes. Evidence may include jewelry and/or vehicles, as well as the contents of storage lockers, safe deposit boxes or bank accounts.

The use of bank accounts is a common money movement technique used by drug traffickers to receive payment for narcotics from customers outside of their geographic region. It is common for a trafficker to use several bank accounts for this purpose simultaneously in an attempt to avoid detection by the financial institutions and/or law enforcement.

c. The use of multiple accounts, and the commingling of illicit funds with legitimate funds in particular, is often part of the plan to conceal the illegal activity or may be part of the overall integration mechanism by which the illicit funds are made to appear as part of the legitimate income so that only a small portion of or even none of the funds from an account are seized.

d. It is a common technique for money launderers to use casinos to launder their illicit proceeds. Money launderers retain the paperwork provided by casinos with respect to cash-out/winnings, in order to disguise their illicit proceeds as gambling winnings.

e. Traffickers of controlled substances and money launderers, and those who assist them, maintain and tend to retain accounts or records of their drug trafficking and money laundering activities, including lists of drug quantities and money owed, telephone records including contact names and numbers, photographs, and similar records of evidentiary value. These items are generally kept in locations where drug traffickers believe their property is secure and will remain undetected from law enforcement, such as inside their homes, vehicles and storage lockers.

f. Traffickers of controlled substances commonly maintain addresses, vehicles, or telephone numbers which reflect names, addresses, vehicles, and/or telephone numbers of their suppliers, customers and associates in the trafficking organization and it is common to find drug traffickers keeping records of said associates in cellular telephones and other electronic devices. Traffickers almost always maintain cellular telephones for ready access to their clientele and to maintain their ongoing narcotics business.

g. Traffickers and money launderers maintain evidence of their criminal activity at locations that are convenient to them, including their residences vehicles, and storage lockers. This evidence often includes more than contraband and paraphernalia and includes financial records, records of property and vehicle ownership, records of property rented, records of post office boxes used to ship and receive contraband and currency, records of other storage facilities used to hide drugs or currency, and other documentary evidence relating to commission of, and proceeds from, their crimes.

h. During the execution of search warrants, it is common to find papers, letters, billings, documents, and other writings which show ownership, dominion, and control of vehicles, residences, and/or storage units.

i. Persons trafficking and using controlled substances commonly sell or use more than one type of controlled substance at any one time.

j. Traffickers frequently maintain items necessary for weighing, packaging, and cutting drugs for distribution. This paraphernalia often includes, but is not limited to, scales, plastic bags, pill presses and cutting/diluting agents and items to mask the odor of drugs

k. Traffickers and money launders often maintain weapons, including guns and ammunition, in secure locations such as their residences and storage lockers, in order to protect their drugs and drug proceeds.

l. Traffickers often have false identification documents and identification documents in the names of others in order to conceal their identities.

m. Traffickers very often place assets in names other than their own, or use fictitious names and identification, to avoid detection and seizure of these assets by law enforcement. Even though these assets are in other persons' names, the traffickers actually own and continue to use these assets and exercise dominion and control over them.

n. Drug trafficking is a cash business, and in order to escape notice from authorities for using unexplained income, or hide excessive cash from illegal activities, traffickers either keep large quantities of cash at home or other secure locations such as a vehicles and storage locker, or convert the cash into other valuable assets, such as jewelry, precious metals, monetary instruments, or other negotiable forms of wealth. Records of such conversions are often stored where a trafficker lives.

o. Illegal drug trafficking is a continuing activity over months and even years. Illegal drug traffickers will repeatedly obtain and distribute controlled substances on a somewhat regular basis, much as any distributor of a legitimate commodity would purchase stock for sale, and, similarly, drug traffickers will have an "inventory," which fluctuates in size depending upon various factors, including the demand and supply for the product. I would expect the trafficker to keep records of his illegal activities for a period of time extending beyond the time during which he actually possesses illegal controlled substances, in order that he can

maintain contact with his criminal associates for future drug transactions, and so that he can have records of prior transactions for which, for example, he might still be owed money, or might owe someone else money. These records are often created in code.

80. Drug dealers and money launderers use cellular telephones as a tool or instrumentality in committing their criminal activity. They use them to maintain contact with their suppliers, distributors, and customers. They prefer cellular telephones because, first, they can be purchased without the location and personal information that land lines require. Second, they can be easily carried to permit the user maximum flexibility in meeting associates, avoiding police surveillance, and traveling to obtain or distribute drugs. Third, they can be passed between members of a drug conspiracy to allow substitution when one member leaves the area temporarily. I also know that it is common for drug traffickers to retain in their possession phones that they previously used, but have discontinued actively using, for their drug trafficking business. Based on my training and experience, the data maintained in a cellular telephone used by a drug dealer is evidence of a crime or crimes. This includes the following:

a. The assigned number to the cellular telephone (known as the mobile directory number or MDN), and the identifying telephone serial number (Electronic Serial Number, or ESN), (Mobile Identification Number, or MIN), (International Mobile Subscriber Identity, or IMSI), or (International Mobile Equipment Identity, or IMEI) are important evidence because they reveal the service provider, allow us to obtain subscriber information, and uniquely identify the telephone. This information can be used to obtain toll records, to identify contacts by this telephone with other cellular telephones used by co-conspirators, to identify other telephones

used by the same subscriber or purchased as part of a package, and to confirm if the telephone was contacted by a cooperating source or was intercepted on a wiretap here or in another district.

b. The stored list of recent received calls and sent calls is important evidence. It identifies telephones recently in contact with the telephone user. This is valuable information in a drug investigation because it will identify telephones used by other members of the organization, such as suppliers, distributors, and customers, and it confirms the date and time of contacts. If the user is under surveillance, it identifies what number he called during or around the time of a drug transaction or surveilled meeting. Even if a contact involves a telephone user not part of the conspiracy, the information is helpful (and thus is evidence) because it leads to friends and associates of the user who can identify the user, help locate the user, and provide information about the user. Identifying a defendant's law-abiding friends is often just as useful as identifying his drug-trafficking associates.

c. Stored text messages are important evidence, similar to stored numbers. Agents can identify both drug associates, and friends of the user who likely have helpful information about the user, his location, and his activities.

d. Photographs and videos on a cellular telephone are evidence because they help identify the user, either through his or her own picture, or through pictures of friends, family, and associates that can identify the user. Pictures also identify associates likely to be members of the drug trafficking organization. Some drug dealers photograph groups of associates, sometimes posing with weapons and showing identifiable gang signs. Also, digital photos often have embedded "geocode" information within them. Geocode information is typically the longitude and latitude where the photo was taken. Showing where the photo was

taken can have evidentiary value. This location information is helpful because, for example, it can show where coconspirators meet, where they travel, and where assets might be located.

e. Stored address records are important evidence because they show the user's close associates and family members, and they contain names and nicknames connected to phone numbers that can be used to identify suspects.

f. It is common for drug traffickers and money launders to use encrypted means of communication, such as WhatsApp, Signal, Wickr, and Telegram, to attempt to avoid detection by law enforcement. It is common for drug traffickers to install and use these apps on their phones in order to make encrypted calls and send encrypted messages.

81. Investigators are seeking authorization under this warrant to search for, seizure, and secure, all cell phones found at the Target Residence.

## VII. BACKGROUND ON THE DARK WEB AND CRYPTOCURRENCY

82. Based on my training, research, education, and experience, and discussions with experienced agents including SA Cheng, I am familiar with the following relevant terms and definitions:

a. The "dark web" is a portion of the "Deep Web " of the Internet, where individuals must use an anonymizing software or application called a "darknet" to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and

transactions are shielded from interception and monitoring. Famous dark web marketplaces, also called Hidden Services, such as Silk Road, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency. Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

c. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

d. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not

issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. Cryptocurrency is not illegal in the United States.

e. Bitcoin ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, bitcoin allows users to transfer

funds more anonymously than would be possible through traditional banking and financial systems.

f. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

g. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of [date], one bitcoin is worth approximately [See www.gdax.com or for daily price], though the value of bitcoin is generally much more volatile than that of fiat currencies.

h. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

i. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18,

2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses. Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

j. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys

that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

83. Based on the information set forth herein, my training and experience, and my discussed with other experienced agents, I believe there is probable cause that, among all the all methods TONG is using to knowingly launder PELAYO's drug proceeds, TONG is also laundering PELAYO's proceeds by purchasing cryptocurrency, such as Bitcoin, with said proceeds. Moreover, I submit that there is probable cause to believe that evidence, fruits and instrumentalities of these violations will be found inside the **Target Residence**.

## VIII. FRUITS, EVIDENCE, AND INSTRUMENTALITIES INSIDE THE TARGET PREMISES AND ANY CLOSED CONTAINERS AND ELECTRONIC DEVICES FOUND THEREIN

84. Through my training, education, and experience, my discussions with experienced agents, including SA Joseph Cheng, I have learned that individuals who engage in the Subject Offenses such as money laundering often keep significant physical evidence, fruits, and instrumentalities of their crimes inside their residences, including, but not limited to, controlled

substances, packaging material and packing inserts (from outgoing drug shipments and incoming cash deliveries), shipping labels (from outgoing drug shipments and incoming cash deliveries), ledgers reflecting drug transactions and funds laundered, drug and financial transaction reports, customer and supplier lists, identification documents and records confirming residency, access devices relating to drug supplies and financial accounts (such as swipe cards to medical offices and credit and debit cards), detailed financial records, and cash proceeds.

85. I have also learned through training, education, and experience that such evidence, fruits, and instrumentalities are often stored in locked containers, safes, secret compartments, closets, drawers, above or below ceiling and floor tiles, behind false walls, and in other places intended to avoid detection by other people, including law enforcement.

86. Finally, I know that the commission of the Subject Offenses in the manner set forth above necessarily requires the use of computers, smart phones, tablets, or other computer devices and storage media for the perpetrator to access dark web marketplaces and cryptocurrency exchanges and wallets, connect with customers, and co-conspirators, and engage in transfers of digital currency. I have learned through training and experience that individuals who engage in the Subject Offenses in this way also commonly use such electronic devices to keep track of suppliers, customers and co-conspirators, keep records of illegal transactions and criminal proceeds, and store copies of online chats, emails, and other data. In addition, I know, based on training and experience that perpetrators maintain copies of software programs and other applications to assist with accessing the dark web and running a vendor account, including, but not limited to, Tor browser software, cryptocurrency client and wallet files, digital signature software and related authentication keys, as well as encryption software and related encryption

keys. In such cases, I know that perpetrators often keep such electronic devices inside their homes. In the case of smart phones, tablets, and laptop computers, perpetrators may also keep such devices on their person, either in their pockets or in containers such as carrying bags, cases, backpacks or protective sleeves.

87. Because TONG's crimes involved the use of cryptocurrency and encryption, the items to be seized could be stored almost anywhere within the **Target Residence**, in both physical and electronic formats. For example, Attachment B seeks cryptocurrency addresses, private keys, recovery seeds, PGP keys, and passwords. These pieces of data comprise long and complex character strings, and in my training and experience I know that many cryptocurrency users write down or otherwise record and store such items because they are too long to commit to memory. As such, these keys, passwords, and addresses may be documented in writing and secreted anywhere within a residence. For all of the foregoing reasons, your affiant respectfully submits that probable cause exists to believe that such records, data, and documents will be found within the **Target Residence**, including in computers or on other devices that store electronic data.

88. Furthermore, I have learned through training, education, and experience and discussions with experienced investigators that computers used in furtherance of criminal activity can hold evidence of the criminal activity months (or even years) after the crime occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.
- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

89. Accordingly, and based on all of the above, I submit that there is probable cause to believe the Target Residence and any closed and/or locked containers found therein will contain evidence, fruits, and instrumentalities of the Subject Offenses, and will also contain devices that will (and will, in and of themselves, constitute) further evidence, fruits, and instrumentalities of the Subject Offenses.

## IX. COMPUTER SEIZURE AND SECURE

90. Investigators are seeking authorization under this warrant to seize and secure all cell phones and digital devices found at the **Target Residence**. Similarly, investigators are

seeking authority under this warrant to search for and secure computers and electronic storage media found at the Target Residence. Following seizure of cell phones, digital devices, computers and electronic storage media in the District of Oregon, investigators will seek a follow-up warrant to analyze same in the Western District of Washington.

91. Based on my training and experience, and my discussions with other experienced investigators, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Electronic Storage media: Electronic Storage media is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

92. As described above and in Attachment B, this application seeks permission to search for and seize evidence, fruits and instrumentalities of the commission of the following crimes: *Conspiracy to Commit Money Laundering*, in violation of 18 U.S.C. §§ 1956, 1957, and 1956(h); *Money Laundering*, in violation of 18 U.S.C. § 1956, and *Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity*, in violation of 18 U.S.C. § 1957, that might be found at **Target Residence** in whatever form they are found.

93. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices such as computers, computer hard drives or other electronic and electronic storage media. For example, evidence of money wire or other transfers between PELAYO and TONG may be found on digital devices. As discussed above, TONG used a computer to engage in wire transfers to PELAYO, as described above. Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

94. Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the **Target Residence,** there is probable cause to believe that evidence, fruits or instrumentalities of the above-listed crimes will be stored on those digital devices or other electronic storage media for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for

months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

95. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or

controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a

digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

96. In most cases, a thorough search of a premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or

months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

97. Because several people may share the **Target Residence** as a residence, it is possible that the **Target Residence** will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

98. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing digital devices such as computers and other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit. Prior to

analyzing any such computers or electronic storage media, investigators will apply for a follow-up search warrant in the Western District of Washington.

## IX. REQUEST RELATING TO APPLE TOUCH ID

99. Based upon my training and experience, and my discussions with other experienced agents, I believe that it is likely that the **Target Residence** will contain at least one Apple brand device, such as an iPhone or iPad. This is because the text messages between PELAYO and TONG were found in the "iMessage" section of PELAYO's phone download. Text messages appear in the "iMessage" section of phone. Based on my training and experience I know that iMessages can only be sent between Apple devices. Accordingly, I believe TONG has at least one Apple device such as a cell phone and/or iPad.

100. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

101. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a

more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

102. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

103. The passcode or password that would unlock the Apple device found during the search of the Premises is not known to law enforcement. Thus, it will likely be necessary to press the fingers of the users of the Apple device found during the search of the **Target Residence** to the device's Touch ID sensor in an attempt to unlock the device for the purpose of securing the Apple devices. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the users is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant. In addition, for the purpose of securing the unlocked Apple device, investigators are requesting authorization to change the password of the unlocked Apple device.

104. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the **Target Residence** to press their fingers against the Touch ID sensor of the locked Apple device found during the search of the Premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID. Based on these facts and my training and experience, it is likely that TONG is one user of the device(s) and thus that his fingerprints are among those that are able to unlock the device via Touch ID.

105. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s) found in the **Target Residence** as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

106. I therefore request that the Court authorize law enforcement to press the finger, including thumb, of ANDREW TONG (if present when this warrant is executed) to the Touch ID

sensor of the device(s), such as an iPhone or an iPad, found at the **Target Residence** for the purpose of attempting to unlock the device(s) via Touch ID in order to search the contents as authorized by this warrant.

## X. CONCLUSION

107. Based on the information set forth herein, there is probable cause to search the above described **Target Residence,** as further described in Attachment A, for evidence, fruits and instrumentalities, as further described in Attachment B, of crimes committed by PELAYO, TONG, and their coconspirators, specifically *Conspiracy to Commit Money Laundering*, in violation of 18 U.S.C. §§ 1956, 1957, and 1956(h); *Money Laundering*, in violation of 18 U.S.C. § 1956, and *Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity*, in violation of 18 U.S.C. § 1957. I therefore request that the Court issue a warrant authorizing a search of the **Target Residence**, described in Attachment A, for the items listed in Attachment B, and the seizure and examination of items as detailed therein.

## XI. REQUEST FOR SEALING

108. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at

////

////

////

this time may cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential witnesses, or otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

JUSTIN HUSSEY
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me this 21 day of October, 2019.

HONORABLE JOLIE A. RUSSO
United States Magistrate Judge